RESEARCH ARTICLE OPEN ACCESS

Securing Data and Providing Privacy Assurance using Revocation in Distributed Cloud Server

C.Surya*, S.Banumathi**, A.Neelavathi***, B.Pooja****, R.Manonmani*****
*(Assistant Professor/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: csurya714@gmail.com
** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: gethcikirena@gmail.com
*** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: neelarjunan@gmail.com
**** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: poojacse7@gmail.com
*****(Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: manokavi2427@gmail.com

----------**********----------

Abstract:

To increase the security issues in a private cloud storage from traitor we propose Encrypting File Sharing And Synchronizing Using Efficient Traitor Tracing And Revocation. It implements the revocation algorithms to block the traitors and generates a traitor tracing technique to trace the presence of the traitors. The proposed methodology is suitable for a private cloud storage which can be modified in future to support public clouds. It propose, if an user uploads his data to a cloud storage server the user will be provided with a private and public key. The public key is used to verify that the user belongs to the concerned private cloud. In case of any abnormal activity the proposed methodology revocates the specific user using IP and MAC addresses and provides the longitude and latitude information to the data owner. In addition pattern matching, SQL injection and anomaly detection are proposed to maintain the privacy and security.

Keywords —**encryption, traitor tracing, revocation, privacy, security, and anamoly detection**.

----------**********----------

I. INTRODUCTION

Cloud computing has provision progressed from a bold vision to massive deployments in various application domains. However, the complexity of technology underlying cloud computing introduces novel security risks and challenges. From an end-user point of view the security of cloud infrastructure implies unquestionable trust in the cloud provider, in some cases corroborated by reports of external auditors. While providers may offer security enhancements such as protection of data at rest, end-users have limited or no control over such mechanisms.

There is a clear need for usable and cost-effective cloud platform security mechanisms suitable for organizations that rely on cloud infrastructure. One such mechanism is platform integrity verification for compute hosts that support the virtualized cloud infrastructure. Several

large cloud vendors have signaled practical implementations of this mechanism, primarily to protect the cloud infrastructure from insider threats and advanced persistent threats. We see two major improvement vectors regarding these implementations.

First, details of such proprietary solutions are not disclosed and can thus not be implemented and improved by other cloud platforms. Second, to the best of our knowledge, none of the solutions provides cloud tenants a proof regarding the integrity of compute hosts supporting their slice of the cloud infrastructure.

To address this, we propose a set of protocols for trusted launch of virtual machines (VM) in IaaS, which provide tenants with a proof that the requested VM instances were launched on a host with an expected software stack.

II. EXISTING SYSTEM

Bring-your-own-device (BYOD) policies and an increasingly mobile devices are changing the requirements for how users want (and need) to access corporate data. The cloud storage service is generally initiated by individual users who store data and download it to sync and collaborate while working on projects. Therefore, more and more cloud-based storage platforms provide file syncing and sharing (FSS) services. These two services introduce new features for enterprise file sharing solution for online collaboration and storage:

A. File sharing:

- it allows the users to not only access files anywhere, anytime and from a variety of endpoint devices, but also collaboratively edit file together;

B. File syncing:

- it is a new online backup mechanism for syncing data across multiple devices, such as a home computer, tablet or smart phone, as well as collaboration and working with teams.

At first, the multi-tenant nature of the cloud is vulnerable to data leaks, threats, and malicious attacks. Therefore, it is important for enterprises to have strong access control policies (such as Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC)) in place to maintain the privacy and confidentiality of data for collaboration with teams. Sometimes cloud providers have access to the data stored in the cloud, and can control access to it by outside entities. When this is the case, the challenge is to maintain the confidentiality of data and limiting privileged user access to it. This can be achieved by encrypting the data before storing it in the cloud, and enforcing legal agreements and contractual obligations with the cloud service provider to ensure protection of data.

III. PROPOSED SYSTEM:

We also work on a corporate FSS service with online collaboration In such work security is a major problem that must be considered for deploying a file syncing and sharing service.It is important for cloud providers to have strong access control policies (such as Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC)) in place to maintain the privacy and confidentiality of data for collaboration with teams. To address these problems, it is necessary to design a construction for hierarchical cryptosystems, considering the new features provided by some recently proposed cryptography technologies such as HIBE, ABE, IBE etc..

We present a new FSS model for player abuse prevention and enhanced protection against unauthorized access. The proposed model uses the hierarchical role-based access control (H-RBAC) model, which is recognized for its support for simplified administration and scalability of collaboration and working with teams. Moreover, the design of this model is generic enough to support other access control policies, such as discretionary access control and multilevel security. We show such a cloud-based FSS model. This model that addresses and incorporates the afore-mentioned authorization requirements can be built using three types of components:

A.Anomaly detection:

This is used for detecting abnormal players. More exactly, it is responsible for monitoring deployed resources and might allocate or release them to ensure the compliance of enterprise-side

existing access control system. The output of this module is some suspected anomaly players.

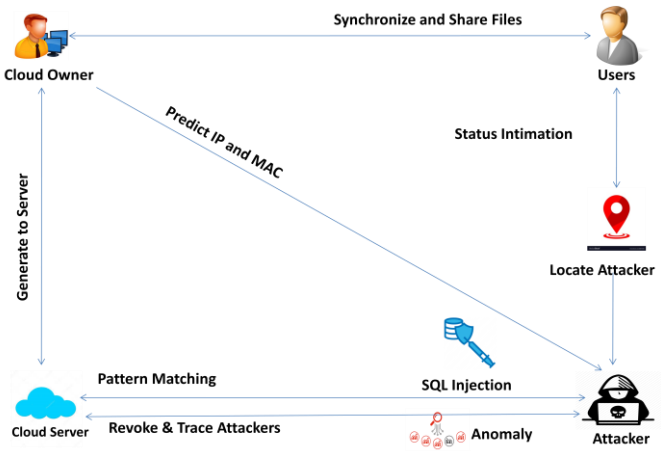
B.Tracing traitors:

This is responsible for finding out the traitors from the suspected players recognized in the previous step. In some cases this is simple and straightforward, but such a practice procedure sometimes results in solution difficulties if we request that the secrets or keys stored in the player cannot be leaked in the tracing procedure. We call it 'black box tracing'.

C.Revoking traitors:

This is responsible for revoking the authority (or license) of traitors found in the previous step. The simple revocation method (e.g., the license is appeared in Blacklist) may be evaded in the way of license forgery and tampering. Taking into account the difficulty in comparing cryptographic key forgery and license forgery, the key based revocation would be a more effective and secure manner.

We implement revocation techniques to block the attackers who the attack the data that has been stored in the cloud storage server. To prevent the data from the intruders we implement various security measures such as Pattern Matching, SQL injection, Traitor Tracing, Anomaly Detection, Revocation



Every mode of entry of attackers has been saved, and blocked the traitors who access the data from the cloud server. So that it blocks the traitors those who try to attack the data. It results in better security and privacy for the data that has been stored in the server and every attackers' IP are traced and revocated. Apart from the specific IP that has been related to the desired cloud owner and the IP that has been added and new entry will be blocked, which enhances the security measures.

IV. CONCLUSIONS

In this paper, we focus on protection the privacy of outsourcing data and preventing player abuse in file syncing and sharing services in the cloud. We highlight the development of a group-oriented cryptosystem with digital forensics, especially for tracing and revoking methods that can ensure the security of player/editor. Based on this cryptosystem, we present a new secure service model to provide a forensic analysis framework to guide investigations.

FUTURE ENHANCEMENT

In our future work, we are planning to introduce a comprehensive anomaly detection using audit attacker identification in public cloud storages, attaining the MAC ID for the every system to enhance the security measure, and also by encrypting the database or the storage that has been allotted to the every cloud user involved in.

REFERENCES

[1] F. R. INSTITUTE, "PERSONAL DATA IN THE CLOUD: A GLOBAL SURVEY OF CONSUMER ATTITUDES," HTTP://WWW.FUJITSU.COM/DOWNLOADS/SOL/FAI/REPORTS/FUJITSU/PERSONAL-DATA-IN-THE-CLOUD.PDF, 2010.

[2] D. QUICK AND K. R. CHOO, "GOOGLE DRIVE: FORENSIC ANALYSIS OF DATA REMNANTS," *J. NETWORK AND COMPUTER APPLICATIONS*, VOL. 40, PP. 179– 193, 2014.

[3] H. CHUNG, J. PARK, S. LEE, AND C. KANG, "DIGITAL FORENSIC INVESTIGATION OF CLOUD STORAGE SERVICES," *DIGITAL INVESTIGATION*, VOL. 9, NO. 2, PP. 81–95, 2012.

[4] D. BONEH AND M. K. FRANKLIN, "AN EFFICIENT PUBLIC KEY TRAITOR TRACING SCHEME," IN *CRYPTO*, 1999, PP. 338–353.

[5] D. BONEH, A. SAHAI, AND B. WATERS, "FULLY COLLUSION RESISTANT TRAITOR TRACING WITH SHORT CIPHERTEXTS AND PRIVATE KEYS," IN *EUROCRYPT*, 2006, PP. 573–592.

[6] Z. LIU, Z. CAO, AND D. S. WONG, "TRACEABLE CP-ABE: HOW TO TRACE DECRYPTION DEVICES FOUND IN THE WILD," *IEEE TRANS. INFORMATION FORENSICS AND SECURITY*, VOL. 10, NO. 1, PP. 55–68, 2015.

[7] D. BONEH AND M. K. FRANKLIN, "IDENTITY-BASED ENCRYPTION FROMTHE WEIL PAIRING," IN *CRYPTO*, 2001, PP. 213–229.

[8] A. SAHAI AND B. WATERS, "FUZZY IDENTITY-BASED ENCRYPTION," IN *EUROCRYPT*, 2005, PP. 457–473.

[9] V. GOYAL, O. PANDEY, A. SAHAI, AND B. WATERS, "ATTRIBUTE-BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA," IN *ACM CONFERENCE ON CCS*, 2006, PP. 89–98.

[10] R. OSTROVSKY, A. SAHAI, AND B.WATERS, "ATTRIBUTE-BASED ENCRYPTION WITH NON-MONOTONIC ACCESS STRUCTURES," IN *ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY*, 2007, PP. 195–203.

[11] S. YAMADA, N. ATTRAPADUNG, G. HANAOKA, AND N. KUNIHIRO, "GENERIC CONSTRUCTIONS FOR CHOSEN-CIPHERTEXT SECURE ATTRIBUTE BASED ENCRYPTION," IN *PUBLIC KEY CRYPTOGRAPHY*, 2011, PP. 71–89.

[12] M. J. ATALLAH, M. BLANTON, N. FAZIO, AND K. B. FRIKKEN, "DYNAMIC AND EFFICIENT KEY MANAGEMENT FOR ACCESS HIERARCHIES," *ACM TRANS. INF. SYST. SECUR.*, VOL. 12, NO. 3, 2009.

[13] M.BLANTON AND K. B. FRIKKEN, "EFFICIENT MULTI-DIMENSIONAL KEY MANAGEMENT IN BROADCAST SERVICES," IN *ESORICS*, 2010, PP. 424–40.

[14] D.BONEH, X. BOYEN, AND E.-J. GOH, "HIERARCHICAL IDENTITY BASED ENCRYPTION WITH CONSTANT SIZE CIPHERTEXT," IN *ADVANCES IN CRYPTOLOGY (EUROCRYPT'2005)*, VOL. 3494 OF LNCS, 2005, PP. 440–456.

[15] S. BERKOVITS, "HOW TO BROADCAST A SECRET," IN *ADVANCES IN CRYPTOLOGY (EUROCRYPT'91)*, VOL. 547 OF LNCS. SPRINGER-VERLAG, 1991, PP. 536–541.

[16] D. BONEH, X. BOYEN, AND E.-J. GOH, "HIERARCHICAL IDENTITY BASED ENCRYPTION WITH CONSTANT SIZE CIPHERTEXT," IN *ADVANCES IN CRYPTOLOGY (EUROCRYPT'05)*, VOL. 3494 OF LNCS, HTTP://EPRINT.IACR.ORG/2005/015, 2005, PP. 440–456.

[17] J.BETHENCOURT, A. SAHAI, AND B. WATERS, "CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION," IN *IEEE SYMPOSIUM ON SECURITY AND PRIVACY*, 2007, PP. 321–334.

[18] D. BONEH AND B. WATERS, "A FULLY COLLUSION RESISTANT BROADCAST, TRACE, AND REVOKE SYSTEM," IN *ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY*, 2006, PP. 211–220.

[19] N. ATTRAPADUNG AND H. IMAI, "CONJUNCTIVE BROADCAST AND ATTRIBUTE-BASED ENCRYPTION," IN *PAIRING-BASED CRYPTOGRAPHY - PAIRING 2009, THIRD INTERNATIONAL CONFERENCE, PALO ALTO, CA, USA, AUGUST 12-14, 2009, PROCEEDINGS*, 2009, PP. 248–265.

[20] A.FIAT AND M. NAOR, "BROADCAST ENCRYPTION," IN *ADVANCES IN CRYPTOLOGY (CRYPTO'93)*, VOL. 773 OF LNCS. SPRINGER-VERLAG, 1994, PP. 480–491.